Iterations in Grover's algorithm and their performance on a Quantum computer

Sarah Ashworth, Hubert Motyka, Ludovica Schaerf and Roberto Caiozzo

June 1, 2020

1 Introduction

Grover's search is undoubtedly one of the most important quantum algorithms. Not only does it provide a solution to a very common problem of unstructured data search, but it also serves both as an instructive example and as a testament to the superiority of quantum algorithms over classical ones. While it is true that like many other quantum algorithms, Grover's search is probabilistic, and thus one can never state with absolute certainty whether the results obtained after its implementation are correct, it nevertheless still represents a quadratic improvement in execution time when compared to the brute force approach. An important result states that the Grover's algorithm is asymptotically optimal, and any other algorithm using the same oracle must perform at least as many iterations as Grover's search [1]. It is not possible to devise an algorithm that would perform the same task in shorter time. Thus a careful analysis of the interrelation between the number of recursive steps and the predicated upon it probabilities associated with the outcome can provide vital insight about the limits of quantum computation.

In this report, we investigate the question of the dependence of confidence of the obtained results on the amount of performed iterations. To this end, we implemented the Grover's search algorithm in the python library Qiskit for the case of two and three qubits, executed it multiple times on both a real and a simulated quantum computer with variable number of iterations, and compared the results. In particular, real quantum systems deal with interactions with the environment an with that introduce noise into the quantum system. This noise can cause discrepancies in the results obtained from real quantum systems. Additional errors can arise due to the depth of the quantum system. Each operation which is applied to a quantum state can lead to minor inaccuracies which accumulate as the number of operations increases [2]. Furthermore, quantum states have a certain coherence time after which the state loses its superposition. This factor can also contribute to the errors observed in the results from real quantum computers.

The unstructured search problem, the solution to which can be determined with high probability with the aid of Grover's algorithm, is to find one particular element in an unsorted (and in principle large) database with the minimum number of queries. One can think of e.g. searching for a given phone number in a phonebook without having any information about its owner. To cast this idea in a mathematical framework, let $a \in \{0,1\}^n$ denote an unknown, marked string of bits to be found, and define a function $f : \{0,1\}^n \to \{0,1\}$, such that

$$f(x) = \begin{cases} 1 & \text{if } x = a \\ 0 & \text{otherwise} \end{cases}$$

Grover's search then proceeds as follows: first, suppose we can construct a unitary operator U, called an oracle and defined as

$$U : |x\rangle |b\rangle \to |x\rangle |b \oplus f(x)\rangle ,$$

where $\oplus$ denotes addition modulo two, and $|b\rangle$ is the oracle qubit which changes its value if and only if $|x\rangle = |a\rangle$. It is useful to choose $|b\rangle = |-\rangle$, which can be achieved with the use of a Hadamard gate applied to state $|1\rangle$. Then

$$U |x\rangle |-\rangle = \begin{cases} |x\rangle |-\rangle & \text{if } f(x) = 0 \\ -|x\rangle |-\rangle & \text{if } f(x) = 1 \end{cases},$$

since $|- \oplus 1\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \oplus 1 = \frac{1}{\sqrt{2}} (|1\rangle - |0\rangle) = -|-\rangle$. The oracle U thus flips the sign of the input state $|x\rangle$ if that state corresponds to the string a, and leaves it unchanged otherwise. It is not hard to see that U can also be expressed in terms of the density matrix, $U = I - 2|a\rangle\langle a|$, where I is the identity matrix, since $(I - 2|a\rangle\langle a|)|x\rangle = I|x\rangle - 2|a\rangle\langle a|x\rangle$. If $|x\rangle \neq |a\rangle$, they are orthogonal and $\langle a|x\rangle = 0$. The action of the oracle can thus be thought of as a reflection of the vector $|x\rangle$ about the normal vector $|a^{\perp}\rangle$ of the hyperplane orthogonal to $|a\rangle$ in a 2^n - dimensional Hilbert space, and U itself functions as a way of distinguishing our marked string $|a\rangle$ from all other possibilities.

However, we still know nothing about $|a\rangle$. In order to determine it, we need to perform the Grover iteration step, which is proceeds as follows. First, prepare a maximally entangled state

$$|\phi\rangle = H^{\otimes n} |0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n} |x_i\rangle ,$$

by a repeated application of the Hadamard gate. The two vectors $|a\rangle$ and $|\phi\rangle$ span a two-dimensional Hilbert subspace of the original 2^n- dimensional state space of n qubits. Then, define another reflection operator R_ϕ, which preserves the sign of $|\phi\rangle$, but flips all other vectors $|x\rangle$ that are orthogonal to $|\phi\rangle$. This can be achieved by setting $R_\phi = 2|\phi\rangle\langle\phi| - I$, as can be readily checked. The next step is to apply $R_\phi U$ to an arbitrary state $|x\rangle$ in the hyperplane spanned by

$|a\rangle$ and $|\phi\rangle$: since the involved operators are linear, the result of this operation is another vector in the same hyperplane. The combination of R_ϕ and U thus corresponds to a rotation of the vector $|x\rangle$ in that hyperplane: firstly by an angle 2δ, where δ is the angle between $|x\rangle$ and $|a^\perp\rangle$, and secondly by 2ϕ, where ϕ is the angle between $U|x\rangle$ and $|\phi\rangle$. The angle $\theta = \delta + \phi$ between $|a^\perp\rangle$ and $|\phi\rangle$ can then be determined from

$$\langle\phi|a\rangle = \frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}} = \cos\left(\frac{\pi}{2} - \theta\right) = \sin(\theta).$$

Thus, each application of the Grover's iterative step rotates the vector $|x\rangle$ in the direction of $|a\rangle$ by the angle of 2θ. For simplicity, suppose now that we choose our initial state to be $|x\rangle = |\phi\rangle$. The result of applying $R_\phi U$ to $|\phi\rangle$ k times is then a vector that is rotated by $\theta + 2k\theta$ with respect to $|a^\perp\rangle$. Thus, in order to find $|a\rangle$, we require $(2k+1)\theta = \pi/2$. For large N, $\sin(\theta)$ is small, and we can approximate it by θ, or $1/\sqrt{N}$. This then gives the optimal number of iterations to be

$$k = \frac{\pi}{4}\sqrt{N} + \frac{1}{2} \approx \frac{\pi}{4}\sqrt{N}.$$

It is not hard to see that Grover's search is a considerable improvement over classical counterparts: since the state space to be searched is of size N, a classical unstructured search algorithm would need to perform (at worst) $N - 1$ queries. A probabilistic algorithm could lower the expected number of queries to $\sim N/2$, but it would still mean $\mathcal{O}(N)$ evaluations of the function f, compared to Grover's $\mathcal{O}(\sqrt{N})$. Grover's search thus represents a quadratic speedup, and due to its lower computational complexity it is superior to any alternative algorithms.

2 Methodology

In order to gain a better understanding of the influence of the number of iterations on Grover's algorithm in real experiments, various simulations and experiments on physical quantum computers were done. All experiments ans simulations were done using the python library Qiskit [3], allowing for the implementation of the produced quantum algorithms in IBM's online quantum computing platform, *IBM Quantum Experience*. This platform offers public access to 5 different quantum systems based on super-conduction [4].

Three main setups were used to gather data and explore the differences between simulated and experiments on a physical quantum computer. The first set up was the quantum circuit of Grover's algorithm for two qubits and a single iteration. Figure 1 shows the used quantum circuit with $|00\rangle$ as the measured string. Similar quantum circuits were built for the three other possible strings ($|01\rangle$, $|10\rangle$, and $|11\rangle$). Each of these circuits was run and measured 1024 times on both a state vector simulator as provided by Qiskit and on the least busy physical quantum computer available through the *IBM Quantum Experience*. One consideration to be made is that this could lead to minor variations. Nonetheless, the noise present in each experiment will likely make these variations negligible.

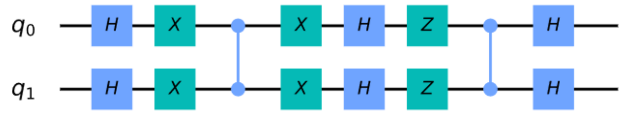

Figure 1: The quantum circuit of Grover's algorithm for two qubits measuring $|00\rangle$

The second and third setups explored the implementation of an additional third qubit on Grover's algorithm on a quantum computer. While a previous study used a single iteration in the study of Grover's algorithm with three qubits [5], in section 1 however we discussed that theoretically 2 iterations offer the most accurate results for three qubits. Thus, the second setup studied was the implementation of Grover's algorithm with 3 qubits and a single iteration and the third setup was the implementation of Grover's algorithm with 3 qubits and two iterations. The setups for the measurements concerned with measuring $|000\rangle$ are given in Figures 2 and 3 respectively. The setups for measuring the 7 other possible strings have also been constructed.

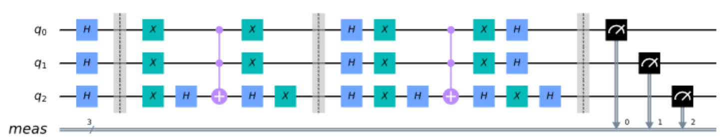

Figure 2: The quantum circuit of the Grover's algorithm for three qubits with a single iteration measuring $|000\rangle$

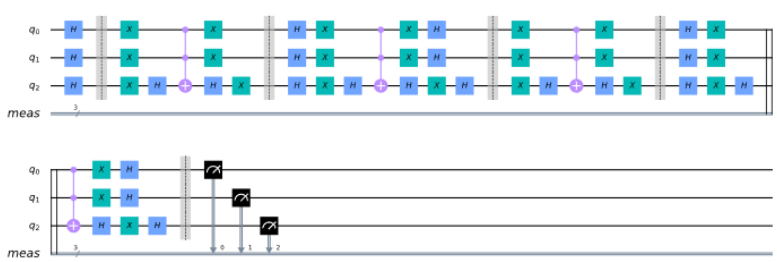

Figure 3: The quantum circuit of the Grover's algorithm for three qubits with two iteration measuring $|000\rangle$

Parallel to the ran experiments for 2 qubits, all setups with 3 qubits ran

1024 times on a state vector simulator and on the least busy physical quantum computer available. Following this the data has been processed and plotted for effective comparison. The following section will set forth the results gathered.

3 Results

This section will first present the results gathered from the 2 qubit circuit of Grover's algorithm (Figure 1), after which it will present the results from the two 3 qubit circuits implemented (Figures 2 and 3).

3.1 Grover's algorithm for 2 qubits

Figure 4 provides the gathered data for the 2 qubit circuit of Grover's algorithm with the 4 different possible strings as the measurements of interest. The simulated outcome yields a total probability of 1 for each of these. The real quantum computer however introduces lower probabilities. Furthermore, it is remarkable that the real experiment of $|01\rangle$ only gave a probability close to 50%. Also, the real experiment of $|11\rangle$ gave a rather low probability close to 75% while the other two experiments yielded probabilities above 90% to measure the right string.

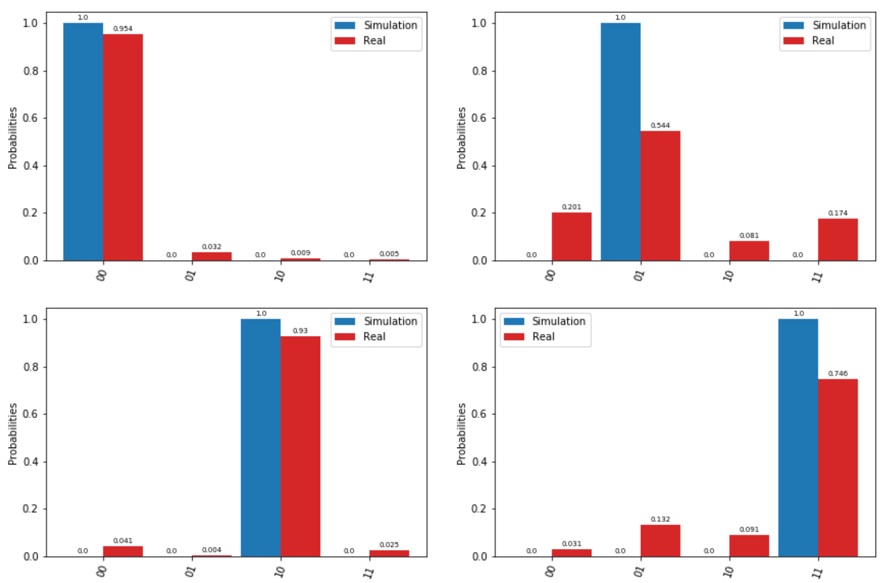

Figure 4: The simulated and experimental results from the quantum circuit of the Grover's algorithm for two qubits with a single iteration measuring $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

One possible explanation for this significant increase of noise is the possible difference in setup between different quantum computers. Noise rises form interactions that the quantum system has with its environment. The real experiments for the measurements of $|01\rangle$ and $|11\rangle$ were done on the quantum computer in Burlington while $|00\rangle$ was done on the quantum computer in Ourense and $|10\rangle$ on the quantum computer in Rome. A different sensitivity to noise that the various quantum computers experience could perhaps help explain this large difference. Furthermore, the depth of the quantum systems and the number of gates implemented differ slightly between the quantum systems. An increase of the depth can reduce the accuracy as the quantum system may face decoherence. Also each operation can introduce additional errors. The circuit for $|11\rangle$ has the lowest depth. But as noise introduced by the different quantum systems can differ over time and per quantum computer majorly it is difficult to determine what the effect of the number of gates its from the results in figure 4.

3.2 Grover's algorithm for 3 qubits

Now turning to Grover's algorithm for 3 qubits, the results for the quantum system with a single iteration are given in Figure 5 and the results for the quantum system with two iterations are given in Figure 6. In Figure 5 we see that simulated values range between 0.76 and 0.799 while measured values range between 0.267 and 0.389. The experimental probabilities thus yield between 30% - 50% of the expected probabilities given by the simulation. For the 2 qubit system the real quantum computer formed a better approximation of the real system as it gave probabilities between 50% - 95% of the expected ones. This increase in the noise could be introduced by the fact that the quantum circuit has a larger depth and allowing for more errors to accumulate and necessitating a longer life time. Furthermore, $|011\rangle$ and $|101\rangle$ were run on the quantum computer in Ourense the other six quantum systems were run on the quantum computer in Melbourne. Nonetheless, no significant difference between their results can be observed.

The probabilities that the 3 qubit system with two iterations gave are presented in Figure 3. The simulated values give probabilities between 0.939 and 0.959 while the physical experiments on the quantum computer range between 0.181 and 0.315. For these experiments $|011\rangle$ and $|111\rangle$ were run on the quantum computer in Ourense while the others were run on the quantum computer in Melbourne. Again no significant difference is notable.

When contrasting these results to that of the 3-qubit system we observe that the simulated values for the quantum circuit with two iterations should yield more accurate results. However, we observe that the probabilities the physical experiments give are slightly smaller for the system with two iterations than those from the system with a single iteration.

To make this difference clearer Figure 7 shows the percentage of the experimentally observed probability with respect to the simulated probability. From these results it is evident that the quantum system for the 3 qubit Grover's algo-

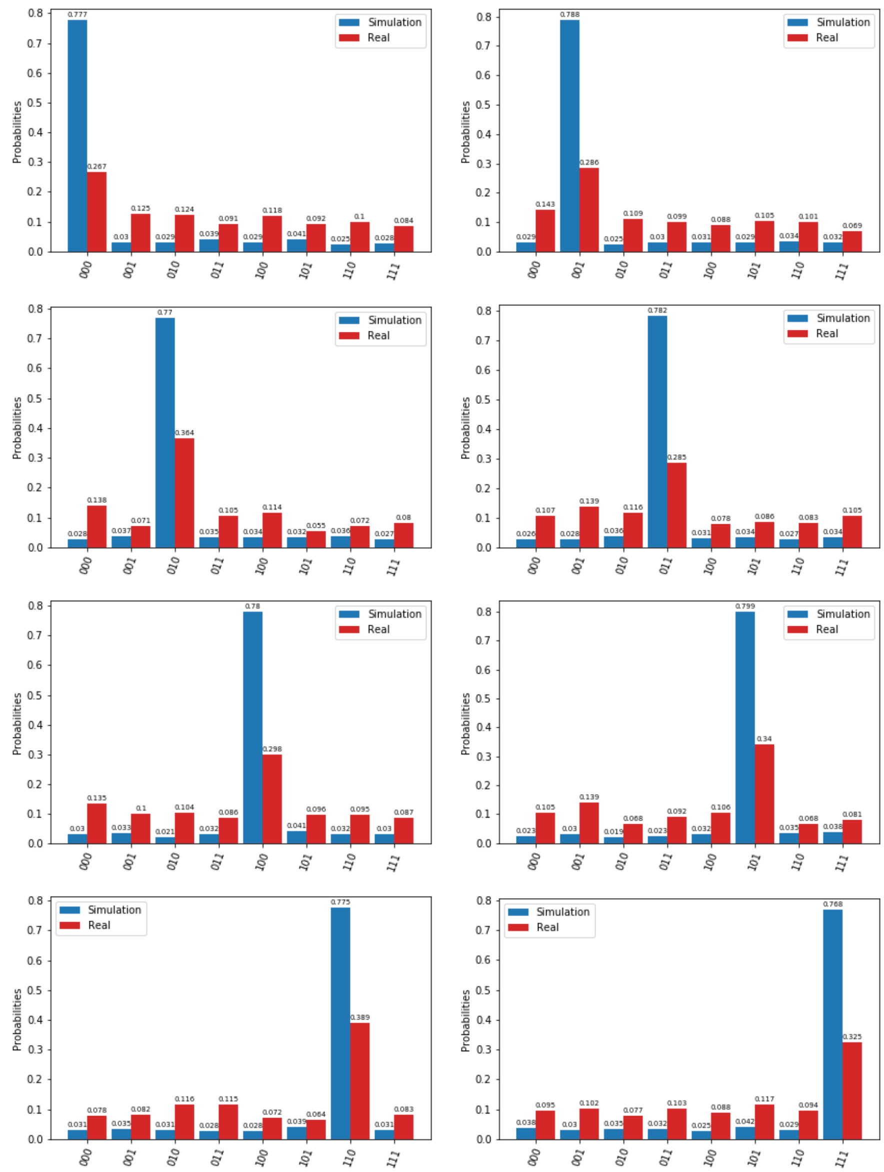

Figure 5: The simulated and experimental results from the quantum circuit of the Grover's algorithm for three qubits with a single iteration measuring $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, and $|111\rangle$.

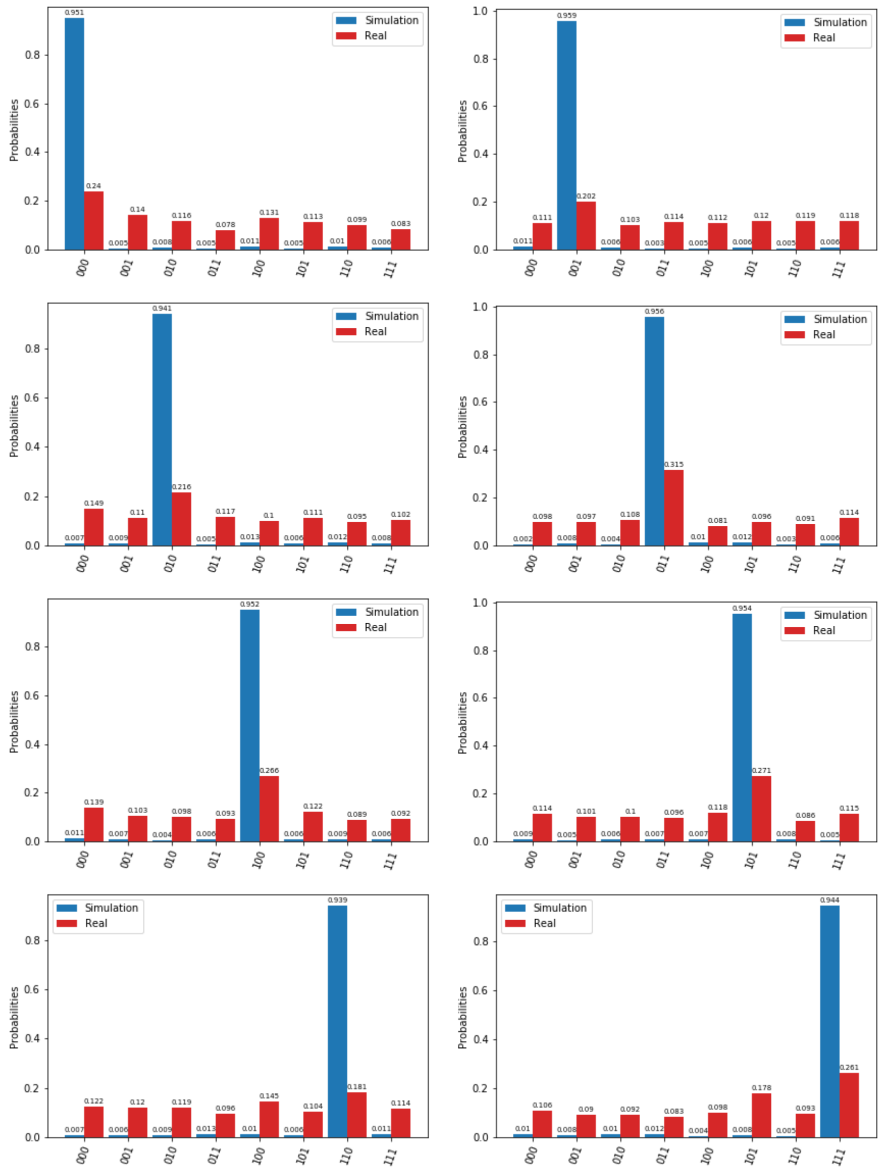

Figure 6: The simulated and experimental results from the quantum circuit of the Grover's algorithm for three qubits with two iterations measuring $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, and $|111\rangle$.

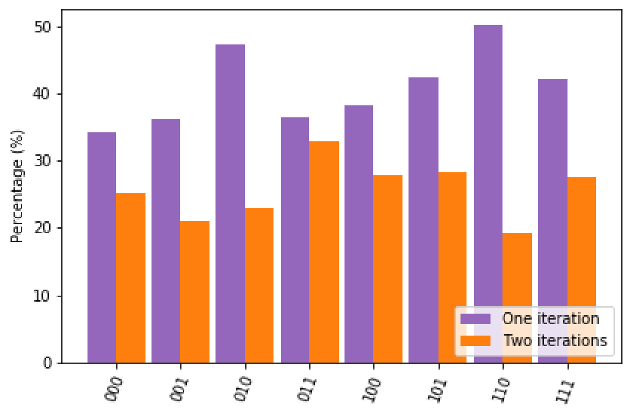

Figure 7: The percentage of the expected simulated value with respect to the experimentally found values for the qubit string of interest. The percentages are given for both one and two iterations of the Grover's algorithm for three qubits.

rithm with one single iteration gives results on a real quantum computer which form a better approximation of the simulated values than those retrieved for the same quantum system with two iterations. This observation can be extended to the absolute probabilities which have shown to be slightly larger for the quantum circuit with one iteration in comparison to the circuit with two iterations. The depths of the respective quantum systems can possible help explain this surprising result. The quantum system with two iterations has a depth which is nearly double the size of the quantum system with a single iteration. Both the number of gates implemented which can introduce errors and the coherence time of the quantum state could play a large role in the major discrepancies observed for the 3 qubit system with two iterations.

4 Discussion and Conclusion

Overall the data collected by running Grover's algorithm on real quantum computers defied our original hypotheses. While in a theoretical framework a second iteration is supposed to improve the accuracy of the results, the real word experiment shows that it is instead actively reducing it and it is likely that for circuits with higher qubits this might lead to null results. Overall noise and decoherence within the quantum computer became a bigger factor then theoretical optimization. This seems to suggest that developing algorithms focused more on reducing the number of computations would be more effective then developing ones focused on idealized conditions.

Another interesting feature of our real world calculations was the difference in results when the algorithm is run on different qubits. This was most evident in the 2 qubits run of the experiment where the success rate ranged from 54.4% to 95.4%. This suggests there might be a systematic error in the circuits setups influencing the results together with the randomized error due to noise and coherence.

Future experiments could explore weather the dominant source of error is the noise source, the depth of the algorithm or the systematic error of the experimental set-up. For example if the result showed a slight increase in measurement for even higher order runs this would suggest the systematic error was dominant. This is because it would mean that for increased runs the angle of the inner product between the solution and the measurement got smaller, which would not happen for increasingly randomized error.

References

[1] Bennet, C. H., Bernstein, E., & Vazirani, U. (1997). The strengths and weaknesses of quantum computation. *SIAM Journal on Computing*, *26*(5), 1510–1523. https://doi.org/10.1137/s0097539796300933

[2] Zhang, Y., Deng, H., Li, Q., Song, H., & Nie, L. (2019). Optimizing quantum programs against decoherence: Delaying qubits into quantum superposition, In *2019 international symposium on theoretical aspects of software engineering (tase)*. IEEE.

[3] Abraham, H., AduOffei, Akhalwaya, I. Y., Aleksandrowicz, G., Alexander, T., Alexandrowics, G., Arbel, E., Asfaw, A., Azaustre, C., AzizNgoueya, Barkoutsos, P., Barron, G., Bello, L., Ben-Haim, Y., Bevenius, D., Bishop, L. S., Bolos, S., Bosch, S., Bravyi, S., ... yotamvakninibm. (2019). Qiskit: An open-source framework for quantum computing. https://doi.org/10.5281/zenodo.2562110

[4] Vu, C. (2016). Ibm makes quantum computing available on ibm cloud to accelerate innovation. *IBM News Room*. https://www-03.ibm.com/press/us/en/pressrelease/49661.wss

[5] Figgatt, C., Maslov, D., Landsman, K., Linke, N. M., Debnath, S., & Monroe, C. (2017). Complete 3-qubit grover search on a programmable quantum computer. *Nature communications*, *8*(1), 1–9.